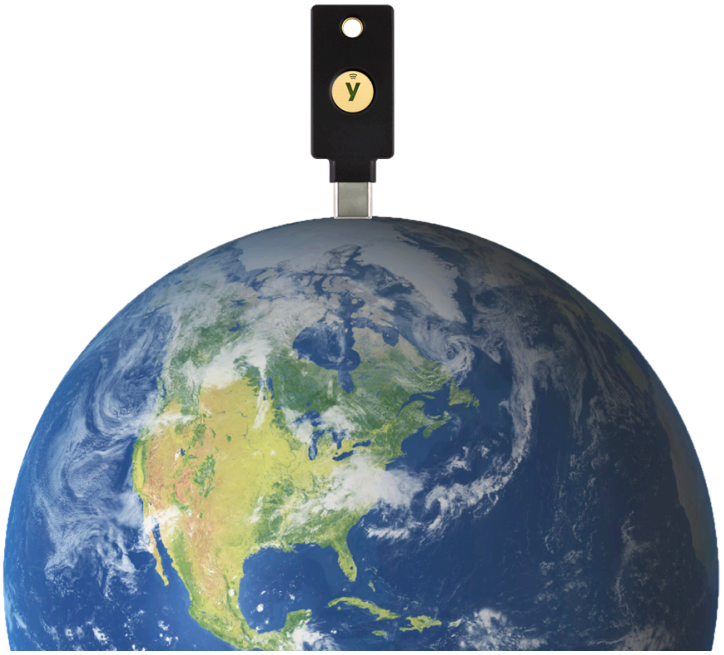
Australian Cyber Security Strategy
Proposed Legislative Reforms

Yubico Response
To Consultation Paper



February 2024

Introduction

Yubico is pleased and impressed by the focus that is being placed by the Australian Government on cyber security. We agree that a resilient national cyber ecosystem is fundamental to a prosperous and viable future. Addressing the cybersecurity challenges in a clear and actionable way is refreshing to see. The Consultation Paper brings together a number of measures that, if acted upon, will reduce the risk of cyber attacks that the nation is up against.

Yubico is a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO[1] Universal 2nd Factor (U2F), FIDO2, WebAuthn, and open authentication standards, and is a pioneer in delivering modern, hardware-based device bound passkey authentication security at scale to customers in over 160 countries.

Yubico appreciates the opportunity to comment on the Consultation Paper and our response focuses on the opportunities that **modern phishing resistant authentication** can provide to improve cyber resilience as part of the national cyber security strategy.

Phishing remains a major challenge

We are all now too familiar with the impact of cyber attacks and the loss of citizen and corporate data. The threat of cyber attacks continues to increase, with ASD Cyber Threat Report 2022-2023[2] stating cyber crime reports have increased 23% and the average cost of cyber crime has increased 14%, with critical infrastructure being a prime target.

Analysis of data breaches and industry research from multiple sources confirm that the majority of data breaches are due to the theft of login credentials, passwords or other weak authentication methods.

- The Verizon 2023 Data Breach Investigations Report[3] cites 81percent of hacking-related breaches are caused by weak or stolen passwords and human-related factors influenced 74 percent of breaches.
- Statista[4] reports that 82 percent of cyber incidents result from human error: clicking on phish links and failing to follow standards.

Common cyber threats, including Ransomware routinely involve a phishing attack to get access to sensitive login credentials.

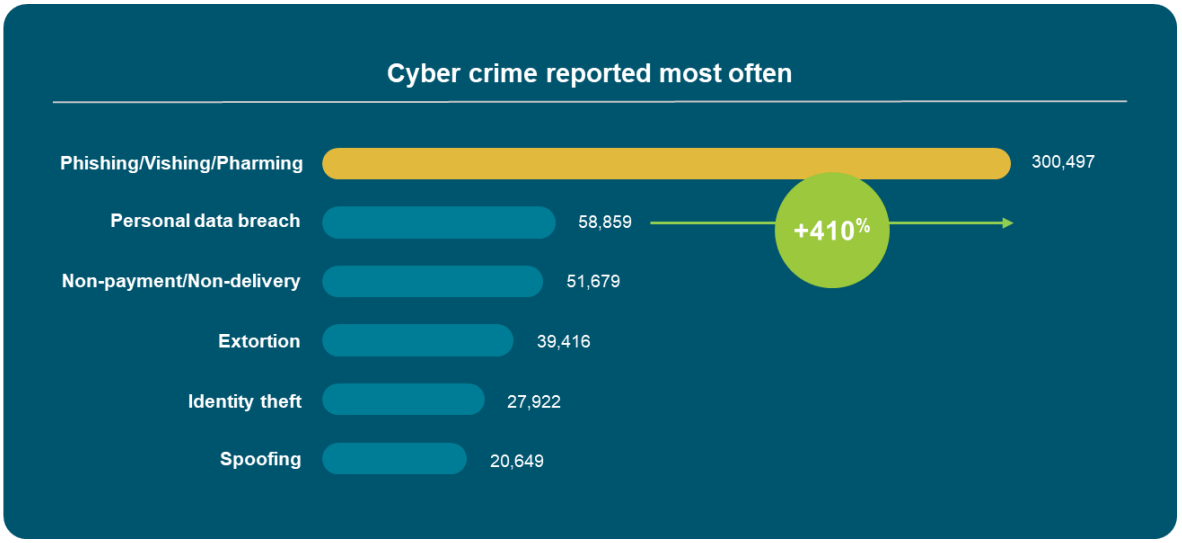


Figure 1 - Statista cyber crime report

So what can we do? There is now a recognition that multi factor authentication (MFA) is required across all of the online services that we use. However, legacy authentication methods are focussed on reusing existing tools to increase security, this has resulted in the failure of organisations to protect their customers' private information and has resulted in major breaches of confidence within Australia and the region. The legacy authentication methods that are predominant within Australia were not designed for security, but they were convenient, and the results are obvious as we see frequent notification of successful data breaches through credential stuffing, phishing or brute force attacks.

The malicious actor realises the financial benefits of data and credential theft and continues to create more sophisticated (now with AI help) environments for users to have their credentials stolen or misused. Once a credential is stolen and MFA compromised, the results can be disastrous for the user and organisation affected.

As we increase our cyber resilience across Australia we must address our most important element in the process, the human, and provide them with secure, simple and readily available login functions that protect their privacy and data to the fullest of our abilities.

Industry leaders, including the Australian Digital Transformation Office as members, have collaborated through the FIDO Alliance[1] to bring modern, human centric authentication paradigms to our digital world in the form of **phishing resistant authentication**.

NIST Special Publication 800-63-B[5] defines phishing resistant authentication as “the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party *without reliance on the vigilance of the subscriber(user)*.

This phishing resistant capability is secure by design and will bring increased user trust in how we engage staff and customers across all digital channels. Simple yet secure authentication will be considered table stakes as we continue to increase delivery of all possible services through digital channels.

A Proactive, Risk Management Approach to Legislation

Current legislative models focus on requirements and obligations for organisations once a cyber incident has been detected. Yubico believes the opportunity exists to introduce legislative changes to require organisations to take a more proactive approach to risk management and in doing so, significantly reduce the risk of a successful cyber attack.

Yubico applauds the work of Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC) in the development and continued enhancement of the Essential 8 guidance for organisations to protect themselves against cyber threats. From the perspective of multi-factor authentication (MFA), Yubico supports the most recent updates to the Essential 8 Maturity Model[6] of November 2023, requiring phishing resistant MFA to comply with Maturity Level 2 and Maturity Level 3.

Our recommended approach for data protection, management and risk mitigation begins by adopting a Zero Trust security model, removing risk and improving usability through adopting phishing resistant authentication capabilities as required by Maturity Level 2 and Maturity Level 3 of the Essential 8.

Protection of our national critical infrastructure against cyber threats should be our highest priority. This must not only include an organisation's internal system users and data repositories, but must also extend to their third party providers and online customer services.

Following the lead of the federal government in announcing support for phishing resistant passkeys on the myGov[6] portal, Yubico believes that all critical infrastructure providers should be required to do the same and offer phishing resistant MFA for their customers. This includes the likes of online banking, customer portals for telecommunications services, energy providers, etc.

Recommendations

Of the nine specific measures outlined in the Consultation Paper, Yubico believes that an opportunity for legislative reform of the Security of Critical Infrastructure (SOCI) Act to move towards phishing resistant authentication is contained within Measure 5 and Measure 8.

Measure 5 - Protecting Critical Infrastructure

Given the important and clear guidance that the Essential Eight Maturity Model provides, Yubico believes that the Security of Critical Infrastructure (SOCI) Act should reference the Maturity Model and require owners and operators of Critical Infrastructure to be at a minimum, a level two maturity.

Referencing the Essential Eight provides a consistent set of guidance that will help organisations more consistently implement the security controls and reduce the risk to data storage systems.

As a case in point, Measure 5 requires owners and operators of Critical Infrastructure to take measures to

- *Increase the cyber maturity of its data storage assets*
- *Introduce more stringent security controls for credentials belonging to third-party service providers*

Given that third-party data breaches are becoming increasingly common as technology makes it easier for businesses to connect and as supply chains grow in complexity, having clear and actionable guidance will be essential. Clearly stating in legislation that organisations need to achieve at a minimum, level two maturity of the Essential Eight will accelerate their efforts to increase their cyber maturity.

Measure 8 - Enforcing critical infrastructure risk management obligations

Consistent with the requirements of Measure 5 to increase cyber maturity, Measure 8 presents the opportunity to legislate for owners and operators of critical infrastructure to take a proactive and consistent approach to risk management in order to significantly reduce the risk of a successful cyber attack.

It is acknowledged that critical infrastructure entities are increasingly taking a more proactive approach to developing their Critical Infrastructure Risk Management Plans (CIRMP). However, the steps and mitigation strategies defined within each entity's CIRMP are not definitive and are open to interpretation. To the point where the Secretary of Home Affairs (or relevant regulator) may deem an entities CIRMP to be seriously deficient.

Referencing the Essential Eight provides a consistent set of guidance that will help organisations more consistently implement their CIRMP. A requirement for owners and operators of Critical Infrastructure to be at a minimum, a level two maturity would provide this consistency.

A positive business case for action

The cost of cyber crime to the Australian economy is significant. The ASD Cyber Threat Report 2022-2023[2] reported that the average cost of cyber crime for businesses was

- small business: $46,000
- medium business: $97,200
- large business: $71,600.

This cost had increased by 14% from the previous report and all indications are that this trend will continue.

Government data for the myGov portal reported scams in 2023 alone that resulted in $3.1 billion in losses from 4,500 scams.

The business case for the nation to act is compelling. This is supported by more detailed analysis in a Forrester report on the Total Economic Impact (TEI) of YubiKeys[8] which found the adoption of phishing resistant MFA delivered significant tangible economic benefits and productivity benefits for end users.

Global Reference - US Federal Government

The most relevant reference for the proactive approach Yubico suggests is the United States White House Executive Order 14028[9] on improving the nation's cyber security and the subsequent Office of Management Budget Memo M-22-09.

In January 2022 the Office of Management and Budget (OMB) set forth a federal Zero Trust Architecture (ZTA) strategy, mandating agencies to meet specific cyber security standards and objectives, including a baseline for access controls across government that prioritised defence against sophisticated phishing attacks.

The memo required federal agency staff, contractors and partners to use phishing resistant multi-factor authentication to reduce the threat from sophisticated attacks. Phishing resistant MFA is required to be used for all authentication, whether in the cloud or on a traditional network. Additionally, the memo expects agencies to use cloud based infrastructure and offer phishing resistant MFA options for public facing digital services.

List of References

1. https://fidoalliance.org/
2. https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023
3. https://www.verizon.com/business/resources/reports/dbir/
4. https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-us/
5. https://pages.nist.gov/800-63-4/sp800-63b.html
6. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-changes
7. https://www.cyberdaily.au/security/9801-mygov-to-move-to-passwordless-authentication-following-reveal-of-3-1b-scam-loss
8. https://www.yubico.com/resource/tei-forrester-report/
9. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based device bound passkey authentication security at scale to customers in over 160 countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.

For more information, please contact:
Mr Geoff Schomburgk
Regional Vice President, Asia Pacific and Japan
[redacted]